REMARKS

Claims 1-2 and 4-18 are pending in this application. Claims 1, 5, 14 and 18 are independent claims. Claims 1-2 and 4-6 are amended. Claim 7-18 are added. Reconsideration and allowance of the present application are respectfully requested.

Entry of Amendment After Final Rejection

Entry of the Amendment is requested under 37 C.F.R. § 1.116 because the Amendment: a) places the application in condition for allowance for the reasons discussed herein; b) does not present any additional claims without canceling the corresponding number of final rejected claims; and/or c) places the application in better form for an appeal, if an appeal is necessary. Entry of the Amendment is thus respectfully requested.

Claim Rejections Under 35 U.S.C. §103

Claims 1-2 and 4-6 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,604,807 to Yamaguchi et al. (hereinafter "Yamaguchi") in view of "Transparent Network Security Policy Enforcement," Keromytis et al. (hereinafter "Keromytis") and in view of U.S. Patent Publication No. 2002/0108043 to Tanaka (hereinafter "Tanaka"). This rejection is respectfully traversed.

Yamaguchi discloses that each client and each cipher gateway device are connected with the key distribution center, the network, and the server in a configuration as shown In FIG. 12. The key distribution center generates the session key, and transmits the generated session key to the cipher gateway device. The network establishes the sessions and carries out the communications between the client and the server, between the key distribution center and the cipher gateway device, and between the client and the cipher gateway device. The client and the server communicate with each other by exchanging packets, while the cipher gateway device enciphers or deciphers the packets exchanged between the client and the server. The client includes a session key distribution unit for making the cipher communication request to the cipher gateway device, and obtaining the session key from the cipher gateway device. The cipher gateway device includes an enciphering/deciphering unit for obtaining the session key from the key management unit by using the session number obtained by the session identifying

unit, and deciphering the packet when it is a packet destined to the server from the client, or enciphering the packet when it is a packet destined to the client from the server. See Col. 10, line 53-Col. 11, line 39 and Col. 13, line 60-Col. 14, line 12 of Yamaguchi.

      Keromytis discloses that network bridges transparently connect two or more LAN segments by storing a frame received from one segment and forwarding it to another segment. Keromytis discloses an Ethernet bridge that also provides IP filtering capability. As Ethernet frames pass through the bridge, they are examined to see if they carry IP traffic. If not, the frame is just bridged. If the frame includes IP traffic, the Ethernet header is removed from the frame and copied and the resulting IP packet is passed to a subroutine which notifies the bridge whether the packet is to be forwarded or dropped. The Ethernet header of the frame under examination is appropriately modified on the frame to be forwarded, and the resulting frame is bridged. Network layer encryption, typically in the form of IPsec, is used to protect traffic between networks, hosts and users. In a virtual LAN Ethernet frames are encapsulated inside IPsec packets and then transmitted to a remote device which removes the protection and forwards the frames to the local LAN. Alternatively, in a "bump in the wire" configuration, a bridge transparently implements IPsec on behalf of one or more hosts.

      Tanaka discloses an audio data and video data decoding apparatus that includes a receiving device that receives partly encrypted MPEG data that is transmitted from a transmitting device. A switch selects the partly encrypted MPEG data. An encryption period/non-encryption period detecting portion inputs the partly encrypted MPEG data and detects whether or not the input MPEG data has been encrypted at each time. A decrypting device inputs the partly encrypted MPEG data and decrypts it using an encryption key extracted from an electronic watermark by an encryption key extracting portion. A switch selects the partly encrypted MPEG data in the non-encryption period or non-encrypted MPEG data that is inputted from the decrypting device in the encryption period on the basis of an encryption period/non-encryption period detection signal that is input from the encryption period/non-encryption period detecting portion. Each of encryption period and the non-encryption period may be assigned to MPEG data in file units or sequence units. However, if a flag that represents the encryption period/non-encryption period is inserted into a private packet of MPEG data or if the non-encryption period is a fixed time period, the encryption period and the non-encryption period may be assigned to

MPEG data in shorter or longer units than file units or sequence units.   FIG. 6 is a timing chart showing operations of the principal portions of the audio data and video data encoding apparatus. See at least paragraphs 0062, 0082-0085 and 0090-0091

Applicants submit that the combination of cited references does not teach or suggest the combination of elements recited in the pending claims.   Independent claims 1, 5, 14 and 18, in part, recite "a manager terminal to input various information into each of the encryption apparatus and the communications terminals having encrypting capability, the information including whether or not data packets are to be discarded between specific terminals after the data packets have been received and a time period for the encryption, thereby completing settings for the encrypted data communications on each of the apparatus and the terminals having encrypting capability." Yamaguchi does not teach or suggest these features.

As noted in the Office Action, Yamaguchi does not teach or suggest "the information including whether or not data packets are to be discarded between specific terminals after the data packets have been received and a time period for the encryption," as recited in the pending claims. Yamaguchi also does not teach or suggest that the manager terminal is to "input various information into each of the encryption apparatus and the communications terminals having encrypting capability," as recited in the pending claims. (underlining added).   Instead, as discussed above, Yamaguchi merely discloses that the key distribution center generates the session key, and transmits the generated session key to only the cipher gateway device.   The cipher gateway device later transmits the key to the client.   Therefore, there is no teaching or suggestion in Yamaguchi that the manager terminal is to "input various information into each of the encryption apparatus and the communications terminals having encrypting capability," as recited in the pending claims.

The Office Action cited Tanaka to cure the some of deficiencies of Yamaguchi. Although Tanaka discloses a time period for encryption, Tanaka does not teach or suggest inputting any "information including whether or not data packets are to be discarded between specific terminals after the data packets have been received," as recited in the pending claims.

Keromytis also does not cure the deficiencies of Yamaguchi. As noted above, Keromytis discloses that if a frame includes IP traffic, the Ethernet header is removed from the frame and copied and the resulting IP packet is passed to a subroutine which notifies the bridge whether the

packet is to be forwarded or dropped at the bridge. In Keromytis, the Ethernet header of the frame under examination is appropriately modified on the frame to be forwarded, and the resulting frame is bridged. Thus, in Keromytis, when the <u>bridge</u> receives the packet, it drops the packet or forwards the packet. There is no teaching in Keromytis of "information including whether or not data packets are to be discarded <u>between specific terminals</u> after the data packets have been received," as recited in the pending claims. In Keromytis, the information is only provided to discard the packet at the bridge, and not to discard the packet "<u>between specific terminals</u> after the data packets have been received," as recited in the pending claims.

Furthermore, Keromytis does not teach or suggest that "the encryption apparatus further includes a bridge to output data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus without any routing process after the encrypting or decrypting process," as recited in claims 1, 14 and 18. As noted above, Keromytis discloses that network layer encryption, typically in the form of IPsec, is used to protect traffic between networks, hosts and users. Keromytis does not discuss whether or not the network layer encryption is performed "without any routing process after the encrypting or decrypting process," as recited in claims 1, 14 and 18.

Keromytis also does not teach or suggest "wherein the encryption apparatus outputs encrypted or decrypted data from another of the plurality of ports through a data link layer and a physical layer associated with the other port without passing said data to a network layer in which routing between networks is controlled," as recited in claim 5. In fact, the teaching of Keromytis seems to be contrary to the elements recited in the pending claims. In particular, Keromytis seems to teach that the bridge outputs encrypted or decrypted data after passing the data to a network layer in which routing between networks is controlled and network IP security is performed.

Keromytis also does not discuss bridging data "received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus without any routing process after the encrypting or decrypting process," as recited in the pending claims. Instead, Keromytis discloses several methods of using IPsec in a bridge, none of which discloses bridging "output data received on one of a plurality of ports of the encryption apparatus to another port of the

encryption apparatus without any routing process after the encrypting or decrypting process," as recited in pending claims.

Based on the distinctions noted above, Applicants submit that the combination of references does not teach or suggest the combination of elements recited in claims 1, 5, 14 and 18. Each of claims 2, 4, 6-13 and 15-17 depends on claims 1, 5 and 14, and incorporates all of the elements of claims 1, 5 and 14, in addition to the further elements recited in claims 2, 4, 6-13 and 15-17. Hence, claims 2, 4, 6-13 and 15-17 are allowable at least because of their dependence on claims 1, 5 and 14. Therefore, Applicants respectfully request that this rejection of claims 1-2 and 4-6 under 35 U.S.C. §103 be withdrawn.

Disclaimer

Applicants may not have presented all possible arguments or have refuted the characterizations of either the claims or the prior art as found in the Office Action. However, the lack of such arguments or refutations is not intended to act as a waiver of such arguments or as concurrence with such characterizations.

CONCLUSION

In view of the above, consideration and allowance are respectfully solicited.

In the event the Examiner believes an interview might serve in any way to advance the prosecution of this application, the undersigned is available at the telephone number noted below.

The Office is authorized to charge any necessary fees to Deposit Account No. 22-0185.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 27592-01101-US1 from which the undersigned is authorized to draw.

Dated: April 21, 2009   Respectfully submitted,

Electronic signature: /Arlene Neal/
Arlene Neal
   Registration No.: 43,828
CONNOLLY BOVE LODGE & HUTZ LLP
1875 Eye Street, NW
Suite 1100
Washington, DC 20006
(202) 331-7111
(202) 293-6229 (Fax)
Attorney for Applicant